Deutscher Bundestag
11. Wahlperiode

Drucksache 11/8197

24. 10. 90

Sachgebiet 204

Änderungsantrag

der Fraktion DIE GRÜNEN/Bündnis 90

zur zweiten Beratung des Gesetzentwurfs der Bundesregierung
— Drucksachen 11/7029, 11/8177 —

Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG)

Der Bundestag wolle beschließen:

1. § 1 erhält folgende Fassung:

„§ 1
Zweck des Gesetzes

(1) Zweck dieses Gesetzes ist es, die Verletzlichkeit der Gesellschaft durch die Nutzung der Informationstechnik zu verringern und insbesondere die Sicherheit der Bürger vor den Gefahren der Informationstechnik zu erhöhen.

(2) Zu diesem Zweck errichtet der Bund ein Bundesamt für die Sicherheit in der Informationstechnik, das die Verletzlichkeit der Gesellschaft durch die Nutzung der Informationstechnik untersucht, bewertet und im Rahmen der ihm zugewiesenen Befugnisse zu ihrer Verringerung beiträgt.

(3) Das Bundesamt für die Sicherheit in der Informationstechnik wird als selbständige Bundesoberbehörde errichtet. Es unterliegt der Rechtsaufsicht des Bundesministers des Innern.

2. In § 2 erhält Absatz 2 folgende Fassung:

„(2) Verletzlichkeit der Gesellschaft im Sinne dieses Gesetzes bedeutet die Möglichkeit großer Schäden für einzelne oder die Gesellschaft, deren Wahrscheinlichkeit oder Schadensausmaß durch die Informationstechnik beeinflußt wird."

Folgender Absatz 3 wird angefügt:

„(3) Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards zur Verringerung der Verletzlichkeit der Gesellschaft durch Vorkehrungen, die

das Ausmaß möglicher Schäden verringern, insbesondere durch

— technische und organisatorische Sicherungsmaßnahmen zur Begrenzung des Schadensausmaßes,
— Katastrophenschutzmaßnahmen,
— Maßnahmen zur Verringerung der Abhängigkeit von informationstechnischen Systemen oder Komponenten,
— Maßnahmen zur Erhaltung funktions-äquivalenter Alternativen zu informationstechnischen Systemen oder Komponenten,

und die die Wahrscheinlichkeit möglicher Schäden verringern, insbesondere durch

— technische und organisatorische Sicherheitsvorkehrungen, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen gewährleisten,
— technische und organisatorische Sicherungsmaßnahmen, die die Verfügbarkeit und Integrität informationstechnischer Systeme und Komponenten gewährleisten,
— die Förderung konsensorientierter Einführungen von Informationstechniken."

3. § 3 wird wie folgt geändert:

a) Nummer 4 erhält folgende Fassung:

„4. Zulassung von informationstechnischen Systemen oder Komponenten, soweit sie im Bereich des Bundes für die Verarbeitung oder Übertragung amtlich geheimgehaltener Informationen (Verschlußsachen) eingesetzt werden sollen."

b) Nach Nummer 4 wird Nummer 4 a eingefügt:

„4 a. Herstellung der für den Betrieb zugelassener Verschlüsselungsgeräte notwendigen Schlüsseldaten, soweit sie im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes für die Verarbeitung oder Übertragung amtlich geheimgehaltener Informationen (Verschlußsachen) eingesetzt werden müssen."

c) Nach Nummer 4 a wird Nummer 4 b eingefügt:

„4 b. Förderung einer unabhängigen Erforschung, Entwicklung und Anwendung von Verschlüsselungssystemen."

d) Nach Nummer 4 b wird Nummer 4 c eingefügt:

„4 c. Untersuchung von Alternativen zu geplanten Informationssystemen durch Auftragsvergabe an unabhängige Forschungseinrichtungen."

e) Nummer 5 erhält folgende Fassung:

„5. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen, ins-

besondere des Bundesbeauftragten für den Datenschutz, mit Ausnahme der Geheimdienste und der Polizeibehörden des Bundes."

f) Nummer 6 (wird ersatzlos gestrichen)

g) Nach Nummer 7 wird Nummer 8 angefügt:

„8. Beratung und Erstellung von Gutachten auf Anforderung des Deutschen Bundestages oder der Bundesregierung."

h) Nach Nummer 8 wird Nummer 9 angefügt:

„9. Sammeln und Dokumentieren von Schadensfällen."

i) Nach Nummer 9 wird Nummer 10 angefügt:

„10. Erstellung eines jährlichen Verletzlichkeitsberichts an den Deutschen Bundestag und die Bundesregierung."

j) Nach Nummer 10 wird Nummer 11 angefügt:

„11. Beteiligung an Genehmigungs-, Zulassungs- und Planungsverfahren, die für die Verletzlichkeit der Gesellschaft durch die Nutzung der Informationstechnik erhebliche Auswirkungen haben können."

4. Nach § 3 wird folgender § 3a eingefügt:

„§ 3a
Anzeigepflichten

(1) Jeder, der informationstechnische Systeme oder Komponenten der Informationstechnik herstellt, errichtet, vertreibt oder betreibt, die erhebliche Auswirkungen auf die Verletzlichkeit der Gesellschaft haben, hat dies dem Bundesamt für die Sicherheit in der Informationstechnik anzuzeigen. In der Anzeige sind insbesondere

— die Konfiguration
— die Funktionen
— die Schadensmöglichkeiten und Schadensfolgen
— die Sicherungskonzepte
— die Notfallplanung und
— die verfügbaren funktionalen Äquivalente

zu beschreiben, damit die Verletzlichkeit der Gesellschaft durch die Nutzung der Informationstechnik in ausreichendem Maße beurteilt werden kann.

(2) Jeder Betreiber, der durch Ausfall, Fehler oder Manipulationen informationstechnischer Systeme oder Komponenten (Störung) nach Absatz 1 einen Schaden erleidet, hat das Ausmaß des Schadens und die näheren Umstände seiner Verursachung unverzüglich dem Bundesamt für die Sicherheit in der Informationstechnik anzuzeigen. In der Anzeige sind insbesondere

— die Ursachen des Schadens,
— die unmittelbaren und mittelbaren Auswirkungen der Störung,

– die Maßnahmen, die zur Verhinderung der Störung, zur Begrenzung seiner Auswirkungen sowie zur Vermeidung von Wiederholungen und zur Verringerung des Schadenspotentials ergriffen worden sind

anzugeben, damit die Störung im Hinblick auf die Verletzlichkeit der Gesellschaft in ausreichendem Maße beurteilt werden kann.

(3) Soweit dies erforderlich ist, damit das Bundesamt für die Sicherheit in der Informationstechnik den Schadensfall bewerten kann, ist der Hersteller, Eigentümer und Verwender von Informationssystemen oder Komponenten verpflichtet, den Mitarbeitern des Bundesamtes über die Schadensmeldung hinaus Auskunft über den Schadensfall, seine Ursachen, sein Ausmaß sowie etwaige Gegenmaßnahmen zu erteilen sowie Einsicht in das betreffende Informationssystem zu gewähren. Artikel 13 GG wird insoweit eingeschränkt.

(4) Die Bundesregierung bestimmt nach Anhörung der beteiligten Kreise durch Rechtsverordnung unter Berücksichtigung der Verletzlichkeit der Gesellschaft und der Bürgersicherheit die informationstechnischen Systeme und Komponenten, die nach Absatz 1 anzeigepflichtig sind, die Schäden, die nach Absatz 2 anzeigepflichtig sind, sowie den Umfang und Inhalt dieser beiden Anzeigepflichten. Beteiligte Kreise sind ein jeweils auszuwählender Kreis aus Vertretern der Wissenschaft, der Wirtschaft sowie der durch die Informationstechnik Betroffenen.

(5) Absatz 1 bis 3 gelten nicht für die Behörden der Länder und Gemeinden. Eine freiwillige Anzeige ist ihnen freigestellt."

5. Nach § 3a wird folgender § 3b eingefügt:

„§ 3b
Dokumentation und Veröffentlichungen

(1) Das Bundesamt für die Sicherheit in der Informationstechnik hat alle eingegangenen Anzeigen nach § 3a zu dokumentieren und auszuwerten. Das Bundesamt führt ein Register über diese Anzeigen. Das Register kann von jedem eingesehen werden.

(2) Die anonymisierten Auswertungen der Anzeigen sind regelmäßig zu veröffentlichen.

(3) Das Bundesamt für die Sicherheit in der Informationstechnik hat die von ihm in Auftrag gegebenen Untersuchungen zu veröffentlichen."

6. Nach § 3b wird folgender § 3c eingefügt:

„§ 3c
Verletzlichkeitsbericht

(1) Das Bundesamt für die Sicherheit in der Informationstechnik beschreibt und bewertet jährlich in einem zusammenfassenden Bericht an den Deutschen Bundestag und die

Bundesregierung die Entwicklung der Verletzlichkeit der Gesellschaft.

(2) In diesem Bericht soll das Bundesamt für die Sicherheit in der Informationstechnik insbesondere die Abhängigkeit der Gesellschaft von informationstechnischen Systemen und das damit verbundene Schadenspotential beschreiben und allen betroffenen gesellschaftlichen und staatlichen Instanzen Vorschläge unterbreiten, wie sie durch Technikgestaltung die Verletzlichkeit der Gesellschaft reduzieren können."

7. Nach § 3c wird folgender § 3d eingefügt:

„§ 3d
Empfehlungen und Anordnungen

(1) Soweit die Sicherheit in der Informationstechnik berührt ist, kann das Bundesamt in Genehmigungs-, Zulassungs- und Planungsverfahren der Behörden und Unternehmen des Bundes zur Bewertung der Sicherheit in der Informationstechnik Empfehlungen zur Reduzierung der Verletzlichkeit abgeben. Von den Empfehlungen des Bundesamtes darf nur begründet abgewichen werden.

(2) Das Bundesamt für die Sicherheit in der Informationstechnik kann im Einzelfall, in dem die Auswirkungen auf die Verletzlichkeit der Gesellschaft in einem unvertretbaren Ausmaß vernachlässigt werden, die zur Verringerung der Verletzlichkeit erforderlichen Anordnungen für die technische oder organisatorische Gestaltung der informationstechnischen Systeme oder Komponenten treffen. Diese Befugnis erstreckt sich nicht auf die Behörden der Länder und Gemeinden."

8. Nach § 3d wird folgender § 3e eingefügt:

„§ 3e
Beirat

(1) Beim Bundesamt für die Sicherheit in der Informationstechnik besteht ein Beirat.

(2) Der Beirat hat die Aufgabe, das Bundesamt in Grundsatzfragen der Sicherheit in der Informationstechnologie zu beraten.

(3) Der Beirat setzt sich zusammen aus:

1. sechs Vertreter/innen der Wissenschaft, und zwar aus den Bereichen der zivilen herstellerunabhängigen Sicherheitstechnik, der Technikfolgenabschätzung und der Sozialverträglichkeit,
2. einem/r Vertreter/in aus dem Kreis der öffentlichen Datenschutzbeauftragten,
3. zwei Vertreter/innen der Hersteller von Informationssystemen und Komponenten,
4. zwei Vertreter/innen der betroffenen Wirtschaftsverbände,
5. einem/r Vertreter/in der Verbraucherverbände,
6. einem/r Vertreter/in der Gewerkschaften,

7. einem/r Vertreter/in von Bürgerrechtsgruppen,
8. einer Vertreterin von Frauengruppen.

Die Geschäftsführung des Beirates liegt beim Bundesamt. Der Beirat tagt unter Vorsitz des Präsidenten des Bundesamtes. Der Präsident des Bundesamtes und der Vertreter nach Nummer 2 hat im Fall der Beschlußfassung nur beratende Stimme. Der Beirat gibt sich eine Geschäftsordnung. Der Beirat bestimmt die Inhalte seiner Arbeit. Er kann vom Präsidenten des Bundesamtes Auskunft über die Tätigkeit und Planungen des Amtes verlangen. Die Mitglieder des Beirates werden auf Vorschlag der in Frage kommenden Verbände und Einrichtungen vom Präsidenten des Bundesamtes berufen."

9. Nach § 5 wird folgender § 5a eingefügt:

„§ 5a
Präsident des Bundesamtes

Der Präsident des Bundesamtes für die Sicherheit in der Informationstechnik wird nach öffentlicher Anhörung der Kandidaten im Ausschuß für Forschung, Technologie und Technikfolgenabschätzung vom Deutschen Bundestag gewählt. Das Vorschlagsrecht liegt bei der Bundesregierung. Er wird für sechs Jahre gewählt. Wiederwahl ist möglich."

10. Nach § 6 wird folgender § 6a eingefügt:

„§ 6a
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig seine Anzeigepflichten nach § 3a nicht erfüllt oder einer Anordnung nach § 3d Abs. 2 nicht nachkommt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu hunderttausend Deutsche Mark geahndet werden."

Bonn, den 24. Oktober 1990

Frau Birthler, Hoss, Frau Dr. Vollmer und Fraktion

Begründung

A. Allgemeines

Die Errichtung eines Bundesamtes für die Sicherheit in der Informationstechnik soll dazu beitragen, die „Verletzlichkeit der modernen Informationsgesellschaft" durch die Nutzung der Informationstechnik zu verringern. Das Problem der Verletzlichkeit beschreibt die Bundesregierung knapp aber zutreffend in den ersten beiden Sätzen ihrer Gesetzesbegründung mit den Worten: „Viele Bereiche von Wirtschaft und Verwaltung sind bereits heute von dem einwandfreien Funktionieren der Informationstechnik abhängig. Mit dem zunehmenden Einsatz der Informationstechnik steigen auch die damit verbundenen Risiken durch unrichtige, unbefugt gesteuerte, fehlende oder rechtsgutgefährdende Informationen."

Dieser richtigen Problembeschreibung wird jedoch der Gesetzentwurf der Bundesregierung nicht gerecht. Er verengt die Problemsicht auf die Sicherheit der Informationstechnik und überträgt dem neu zu gründenden Amt lediglich Aufgaben und Befugnisse zur Verbesserung der technischen Sicherheit. Um die Verletzlichkeit zu verringern, sind darüber hinaus jedoch die Schadenspotentiale, die durch die Abhängigkeit von der Informationstechnik für die Gesellschaft und den einzelnen Bürger geschaffen werden, die konkreten Anwendungsbedingungen und die durch sie verursachten sozialen Folgen zu berücksichtigen.

Das Problem der Verletzlichkeit, nämlich die Möglichkeit großer Schäden für einzelne oder die Gesellschaft, entsteht vor allem dadurch, daß soziale Funktionen von Menschen auf Informations- und Kommunikationssysteme übertragen werden. Informationsverarbeitung und Kommunikation werden dadurch vom Funktionieren einer Technik abhängig, auf die sich die Menschen verlassen. Im Vertrauen auf die Technik erhöhen sie deren Leistungsfähigkeit – und damit zugleich das Schadenspotential. Durch diese Übertragung werden zudem Informationsverarbeitungs- und Kommunikationsprozesse für Dritte zugänglich. Sie können diese leichtfertig oder mißbräuchlich ausforschen, manipulieren, unterbinden, beschädigen oder zerstören. Fehler und Manipulationen können so die Erfüllung der dem technischen System übertragenen gesellschaftlichen Funktionen beeinträchtigen.

Die Abhängigkeit der Gesellschaft vom Funktionieren der Informationstechnik wird zum Beispiel an der Steuerung der Daseinsvorsorge deutlich. Existentielle Voraussetzung für das Überleben in einer hochindustrialisierten Gesellschaft ist die Bereitstellung von Nahrung, Energiedienstleistungen, Kleidung, Fortbewegungs- und Zahlungsmitteln sowie andere Güter und Dienstleistungen zur Befriedigung der Grundbedürfnisse. Bereits heute, jedenfalls aber in Zukunft werden gerade diese sozialen Funktionen ausnahmlos mit Hilfe von Informationstechnik gesteuert und sind von ihrem Funktionieren vollständig abhängig. Hohe Schadenspotentiale können durch die Abhängigkeit von informationstechnischen Systemen unter anderen in folgenden wichtigen gesellschaftlichen Bereichen entstehen:

– Die Anforderungen an die Zuverlässigkeit, Schnelligkeit und Pünktlichkeit aller Verkehrssysteme nehmen aufgrund von Mobilitätsanforderungen, Just-In-Time-Produktionskonzepten und eng geplanten Vertriebsstrukturen in Warenwirtschaftssystemen zu. Der Ausfall der dort zunehmend eingesetzten informationstechnischen Systeme kann sehr große volkswirtschaftliche Schäden zur Folge haben und die Versorgung der Bevölkerung beeinträchtigen.
– Der Einsatz von Informationstechnik in der Prozeßsteuerung kann durch Automatisierung einerseits Risiken vermindern. Gleichzeitig kann durch engere Kopplung oder größere Produktionsanlagen das Schadenspotential vergrößert werden.
– Manipulationen oder Ausfälle von elektronischen Zahlungssystemen können zu großen volkswirtschaftlichen Schäden führen, einzelne Menschen oder Unternehmen ruinieren und zu Versorgungsengpässen führen.

— Die Gesellschaft ist auf eine stetige, wirksame und kalkulierbare Verwaltung existentiell angewiesen. Ihr Ausfall durch das Versagen von Informationstechnik kann leicht zu großen Schäden für gesellschaftliche Gruppen führen.

Eine weitere Ursache für das Entstehen großer Schäden können Wechselwirkungen zwischen verschiedenen Anwendungsbereichen oder die gemeinsame Nutzung von Basistechniken oder informationstechnischen Infrastrukturen sein. Eine solche enge Kopplung, wie sie beispielsweise durch die fast ausschließliche Verwendung eines Telekommunikationsnetzes entstehen könnte, muß durch entsprechende bereichsübergreifende Planungen vermieden werden. Das künftige Bundesamt könnte in diesem Sinne die Abhängigkeiten, die weder vom Netzbetreiber noch von den Nutzern erkannt werden, analysieren und für eine ausreichende Diversifikation Sorge tragen.

Um die Verletzlichkeit zu verringern, genügt es nicht, lediglich entwicklungsbegleitend einheitliche Sicherheitsstandards herzustellen, informationstechnische Sicherheitskomponenten und -systeme zu erforschen und zu entwickeln sowie die Anwender und Hersteller von informationstechnischen Produkten zu beraten, die informationstechnische Entwicklung aber als unbeeinflußbar hinzunehmen. Vielmehr ist es erforderlich, die Schadenspotentiale, die durch die steigende Abhängigkeit von der Informationstechnik anwachsen, in den Blick zu bekommen und gestaltend zu beeinflussen. Die Aufgaben und Befugnisse des Bundesamtes für die Sicherheit in der Informationstechnik müssen daher darauf abzielen, die Abhängigkeit und die Schadenspotentiale zu erkennen, ein öffentliches Bewußtsein für diese zu schaffen, Gegenmaßnahmen zu untersuchen und zu erproben und die Hersteller und Anwender auf verletzlichkeitsreduzierende Gestaltungsmöglichkeiten hinzuweisen.

B. Einzelvorschriften

1. Zu § 1:

a) Zu Absatz 1:

Der Zweck des Gesetzes ergibt sich aus der oben unter A. dargelegten Zielsetzung.

Der Begriff der Verletzlichkeit der Gesellschaft ist in § 2 Abs. 2 definiert. Eine allein auf die technische Sicherheit bezogene Zwecksetzung wird dem Problem der zunehmenden Abhängigkeit einzelner und der Gesellschaft insgesamt vom Funktionieren informationstechnischer Systeme nicht gerecht.

Diese Erkenntnis führt für die Zwecksetzung des Gesetzes, für den einzelnen und die Gesellschaft ein höheres Maß an Sicherheit zu gewährleisten, zu zwei Folgerungen:

Zum einen ist nicht nur ein technisches System oder eine technische Komponente zu analysieren und zu bewerten, sondern auch dessen soziale Funktion im Rahmen einer konkreten Anwendung. Denn nur so kommen die Abhängigkeit des einzelnen oder der Gesellschaft von der Technik und die mit einem Funktionsversagen verbundenen Schadenspotentiale in den

Blick. Daher ist es notwendig, die informationstechnischen Systeme auch in Sicherheitsanalysen als sozio-technische Systeme zu betrachten.

Zum anderen ist nicht nur die Sicherheit von Geräten und Softwareprodukten zu verbessern. Vielmehr sind vor allem Handlungskonzepte zu entwerfen,

- um die gesellschaftliche Abhängigkeit von Systemen der Informationstechnik zu verringern,
- um die potentiellen Schäden eines Mißbrauchs oder Fehlers der Informationstechnik und die sozialen Folgen eingetretener Schäden zu vermindern,
- um zu verhindern, daß durch die Techniknutzung neue Mißbrauchsmotive hervorgerufen werden,
- um auszuschließen, daß die Informationstechnik neue Mißbrauchsmöglichkeiten und Fehlerquellen eröffnet, und zu erreichen, daß sie bestehende reduziert,
- um zu verhindern, daß die unvermeidlichen Sicherungsmaßnahmen negative Folgen für die Grundrechtsausübung des einzelnen und das soziale und politische System insgesamt hervorrufen.

In den Blick zu fassen sind daher nicht nur die Risiken, die aus Sicherheitsmängeln technischer Produkte entstehen, sondern auch die Risiken, die von den sozialen Bedingungen und Folgen der Informationstechnik-Nutzung und -Sicherung im betrieblichen und gesellschaftlichen Kontext hervorgerufen werden. Und als Risiken dürfen nicht nur die Ausfallkosten eines defekten Techniksystems, der Verrat militärischer Geheimnisse, die finanziellen Verluste durch Computerkriminalität oder verminderte Exportchancen verstanden werden. Als Risiken sind auch und vorwiegend die Nachteile zu betrachten, die dem einzelnen Bürger sowie der Gesellschaft durch den Ausfall der auf die IuK-Technik übertragenen sozialen Funktionen (Verkehr, Energieversorgung, Prozeßsteuerung, Handel, Zahlungsverkehr usw.) entstehen. Außerdem sind die negativen Folgen zu begreifen, die sowohl durch die möglichen Schäden als auch durch die Sicherungsmaßnahmen zu ihrer Verhinderung für die Ausübung von Grundrechten und einen freien Prozeß politischer Willensbildung entstehen können.

Das Bundesamt für die Sicherheit in der Informationstechnik hat als einen wesentlichen Beitrag zur Verringerung der Verletzlichkeit, die Sicherheit der Bürger gegenüber den Gefahren der Anwendungen der Informationstechnik zu erhöhen. Es darf nicht nur die Sicherheitsinteressen großer Institutionen oder der staatlichen Behörden verfolgen oder die Gewährleistung der inneren und äußeren Sicherheit des Staates in den Vordergrund stellen. Damit würde die Bewältigung der Risiken, die für jeden einzelnen Bürger aus der allgegenwärtigen Anwendung der Informationstechnik erwachsen, diesem selbst überlassen. Er müßte der Durchsetzungsmacht „der Großen" erliegen, wenn nicht auch seine Ziele institutionalisiert gegenüber Exekutive und Wirtschaft vertreten würden. Die Gewährleistung von Sicherheit muß daher vor allem

darauf zielen, die Freiheitsgrundrechte der Bürger zu sichern. Der Gesetzentwurf sieht in diesem Sinne jedoch nur die widersprüchliche Unterstützung sowohl des Datenschutzbeauftragten als auch der Sicherheitsbehörden vor.

Für den Bürger bestehen drei zentrale Schutzziele. Er soll zum ersten als Nutzer der Informationstechnik für seine Bedürfnisse keine Risiken in Kauf nehmen müssen. Zum zweiten ist eine gegen seine Interessen gerichtete Nutzung der Technik oder seiner Daten durch staatliche oder private Organisationen zu verhindern. Drittens sind seine Rechte auf informationelle und kommunikative Selbstbestimmung sowie sein Fernmeldegeheimnis gegen das steigende Ausforschungsinteresse staatlicher Sicherheitsbehörden zu schützen:

Das Vorhaben, Softwareprodukte hinsichtlich ihrer Sicherheit und Verfügbarkeit zu bewerten und die Prüfergebnisse durch Zertifikate bekanntzumachen, kann die Markttransparenz im Sinne des Konsumentenschutzes verbessern. Nachhaltig verbessert würde der Verbraucherschutz allerdings erst, wenn etwa strenge Haftungsregelungen an die zertifizierten Eigenschaften geknüpft würden. Hierfür ist jedoch eine eigenständige Regelung vorzusehen.

Durch die immer größeren Sammlungen personenbezogener Daten und die verbesserten Möglichkeiten der Übermittlung und Auswertung wird es immer dringlicher, den Betroffenen von Informationstechnik-Anwendungen zu schützen. Die Transparenz des Kundenverhaltens wird durch die „Informatisierung der Kundenschnittstelle" z. B. bei elektronischen Bestellungen, Kreditanträgen oder der Kundenidentifizierung beim elektronischen Zahlungsverkehr stetig weiter erhöht. Marketingstrategen versuchen mit den gewonnenen Profilen, das Verbraucherverhalten zu beeinflussen. Über die im Gesetz vorgesehene technische Unterstützung des Datenschutzbeauftragten hinaus müßte gerade das BSI die Entwicklung technischer Komponenten vorantreiben und sicherstellen, die – wie auf dem Wochenmarkt – anonyme Teletransaktionen ermöglichen.

In der ‚Informationsgesellschaft' erfolgen erheblich mehr Lebensäußerungen über Netze und werden über jeden bedeutend mehr Daten gespeichert als heute. Dadurch sind die Verhaltensweisen und Lebensgewohnheiten eines jeden in breitem Umfang und in größerer Tiefe einem elektronischen Zugriff offen. Durch die Fortschritte bei der Sprach-, Sprecher- und Bilderkennung ist zu erwarten, daß die Möglichkeiten zur Auswertung von Nutzdaten der Telekommunikation erheblich verbessert werden. Zugleich werden durch die gegenwärtigen Planungen von Telekommunikationsdiensten, z. B. die Digitalisierung des Fernsprechnetzes und ISDN, Möglichkeiten des Zugriffs auf Nutz- und Verbindungsdaten eröffnet. Während die Transparenz des Bürgers für die Sicherheitsbehörden zunehmen wird, dürfte deren Transparenz für die Bürger sinken. Niemand wird mehr in der Lage sein zu wissen, wo überall Daten über ihn gespeichert sind. Noch viel weniger kann er wissen, wie diese interpretiert und wann und wo gegen ihn verwendet werden können.

Der Gesetzentwurf betont jedoch einseitig die Sicherung der Datenverarbeitung bei staatlichen Stellen und die Verfolgung und Verhütung von ‚Computerdelikten'. Der mögliche Mißbrauch von informationstechnischem Systemen durch staatliche Stellen oder Machtverschiebungen zwischen Bürger und Staat durch Technik-Nutzung werden nicht zum Bedrohungspotential gerechnet, gegen das Vorkehrungen zu treffen sind. Im Hinblick auf ihre verfassungsrechtliche Aufgabenstellung darf die Bundesregierung aber Sicherheit nicht auf ‚innere' oder ‚Staatssicherheit' beschränken. Vielmehr muß in einem Rechtsstaat Sicherheit sogar vorrangig Sicherheit der Bürgergrundrechte vor staatlichem Machtmißbrauch bedeuten.

b) Zu Absatz 2:

Die Übertragung der Rechtsaufsicht auf den Bundesminister des Innern bedeutet, daß er keine sachlichen Weisungen erteilen darf, sondern nur die Rechtmäßigkeit des Handels des Bundesamtes für die Sicherheit in der Informationstechnik überwacht. Das Bundesamt für die Sicherheit in der Informationstechnik ist damit weisungsfrei.

2. Zu § 2:

a) Zu Absatz 1 (unverändert)

b) Zu Absatz 2:

Verletzlichkeit ist ein Begriff, der auf das Versagen der sozialen Funktion bezogen ist, die auf informationstechnische Systeme übertragen sind. Er thematisiert daher nicht nur den Ausfall, den Fehler oder die Manipulation eines technischen Systems, sondern auch deren Voraussetzungen und Folgewirkungen.

Der Begriff der Verletzlichkeit enthält zwei ihre Größe bestimmende Bestandteile: das Ausmaß eines Schadens und die Möglichkeit seines Eintritts.

Schaden ist jede nachteilige Veränderung von Rechtsgütern und rechtlich geschützten Interessen. Das Ausmaß des Schadens hängt ab von den gesellschaftlichen Funktionen, die auf die Technik übertragen werden. Mit der Technik kann dann im schlimmsten Fall auch diese soziale Funktion ausfallen. Die Wahrscheinlichkeit des Schadenseintritts kann dadurch beeinflußt werden, daß informationstechnische Systeme und Komponenten die Möglichkeit von Fehlern und Mißbrauch erhöhen oder neue derartige Möglichkeiten schaffen.

c) Zu Absatz 3:

Wird als zentrale Aufgabe des zu schaffenden Bundesamtes angesehen, die Verletzlichkeit der Gesellschaft zu verringern, dann kann Sicherheit nicht – wie im Regierungsentwurf – allein als Übereinstimmung mit technischen Standards verstanden werden. Wenn auch im vorliegenden Gesetzentwurf Sicherheit deterministisch definiert wird, so sind die Standards, denen die zu bewertenden informationstechnischen Systeme und Komponenten entsprechen sollen, auf die Verletzlichkeit der Gesellschaft zu be-

ziehen. Um diese zu verringern, besteht aber ein wesentlich erweiterter Handlungsbedarf mit anderen Schwerpunktsetzungen als im Regierungsentwurf vorgesehen. Hierfür ist die technische Sicherung von informationstechnischen Systemen ein wichtiger, aber keineswegs ausreichender Beitrag.

Die Verletzlichkeit der Gesellschaft ergibt sich aus ihrer Abhängigkeit von der Informationstechnik und den daraus erwachsenden Risiken großer Schäden. Das Ziel eines Bundesamtes, das die Verletzlichkeit vermindern soll, muß es daher sein, gleichermaßen große Schadenspotentiale durch eine hohe Abhängigkeit von Technik-Systemen zu vermeiden und die Wahrscheinlichkeit eines Ausfalls der auf die Technik übertragenen sozialen Funktionen zu vermindern.

Zur Begrenzung der Schadenshäufigkeit trägt es bei, wenn versehentliche Fehler in der Produktion von Hardware und Software sowie bei der Bedienung der Systeme vermieden und mutwilliger Mißbrauch verhindert werden können. Dies kann zum Teil durch die Entwicklung von Prüfkriterien und -verfahren sowie Sicherheitsstandards erreicht werden, wenn sie eine entsprechende Marktnachfrage stimuliert. Allerdings sind hierbei auch Fragen der Beherrschbarkeit durch unvorhersehbare Systemfehler zu berücksichtigen. Gleichzeitig ist durch die Veröffentlichung und Diskussion das Sicherheitsbewußtsein von Anwendern und Herstellern zu schärfen, so daß mittelfristig eine Anpassung der Systeme an die so erkannten Sicherheitsprobleme erfolgen kann.

Dennoch werden diese Maßnahmen nicht alle Fehler- und Mißbrauchsmöglichkeiten ausschließen. Denn insbesondere gegen Insider werden rein technische Vorkehrungen unzureichend sein und die technische Verhinderung von externen Angriffen setzt eine organisatorische und technische Lückenlosigkeit des Sicherungssystems voraus, die in den meisten Fällen in der Praxis nicht zu gewährleisten ist. Für eine umfassende Bewertung der Technik und ihrer Folgen ist deshalb auch die Verläßlichkeit von technischen Sicherungsvorkehrungen und die aus Defiziten folgenden ergänzenden personenbezogenen Sicherungsmaßnahmen zu berücksichtigen. Die aus dem Sicherungszwang resultierenden sozialen Kosten in Form von Grundrechtseinschränkungen müssen in die Bewertung einbezogen werden und zu sozialverträglichen Sicherungskonzeptionen führen.

Sicherheit in der Informationstechnik setzt weiter voraus, Motive für Angriffe gegen umstrittene Informationstechnik-Systeme zu vermindern und deshalb eine konsensorientierte Technikeinführung anzustreben. Dies ist aber nur auf der Basis einer frühzeitigen und breiten Beteiligung der Betroffenen zu erreichen.

Als vorrangige Aufgabe zur Herstellung von Sicherheit muß jedoch die Begrenzung des Schadenspotentials angesehen werden. Denn nur dann werden hohe Sicherungszwänge vermieden und kann auf die Einschränkung der Freiheitsgrundrechte von Bedienern und Bürgern zur organisatorischen Sicherung der Technik verzichtet werden. Für die verschiedenen Anwendungen von Informationstechnik sollte demnach das Bundesamt jeweils

prüfen, welche Abhängigkeiten durch den Technikeinsatz entstehen. Im konkreten Fall sind dazu verschiedene Alternativen des Technikeinsatzes zu vergleichen und hinsichtlich der Folgen für die Gesellschaft und ihres Schadenspotentials zu bewerten. Insbesondere ist zur Schadensbegrenzung darauf zu achten, daß Substitutionsmöglichkeiten erhalten bleiben, die bei einem Technikausfall zumindest einen „Notbetrieb" gewährleisten. Eine ähnliche Wirkung wird erreicht, wenn die Diversifikation von eingesetzten informationstechnischen Systemen garantiert ist. Durch Softwarefehler oder Manipulation sind dann immer nur einige und nicht alle Anwender betroffen.

3. Zu § 3:

a) Nummer 1 (unverändert)

b) Nummer 2 (unverändert)

c) Nummer 3 (unverändert)

d) Zu Nummer 4

Die Neufassung des Absatzes 4 des Regierungsentwurfs stellt sicher, daß sich die Aufgabe der Zulassung informationstechnischer Systeme oder Komponenten auf den Bereich der Bundesbehörden bzw. auf Unternehmen, die im Rahmen von Aufträgen des Bundes tätig werden, beschränkt.

e) Zu Nummer 4 a

Die eingefügte Nummer 4 a nimmt den letzten Halbsatz der Nummer 3 des Regierungsentwurfs auf und beschränkt die Herstellung der Schlüsseldaten auf die Verarbeitung oder Übertragung von Verschlußsachen. Im Gegensatz zum Regierungsentwurf bezieht sich die Aufgabe der Herstellung von Schlüsseldaten aber nur auf den Bereich des Bundes bzw. auf die für den Bund tätigen Unternehmen. Diese Aufgabenbeschränkung soll zur Reduzierung der Verletzlichkeit der Gesellschaft beitragen. Damit wird sichergestellt, daß das Bundesamt für die Sicherheit in der Informationstechnik die Schlüsseldaten ausschließlich für die Verschlüsselung von Verschlußsachen herstellt und die Entwicklung selbständiger ‚ziviler' Verschlüsselungsmechanismen nicht behindert.

f) Zu Nummer 4 b

Bürgersicherheit kann in der Informationsgesellschaft jedoch nur gewährleistet werden, wenn der Bürger selbst in ausreichendem Maße seine Anonymität wahren und für ihn wichtige Nachrichten vor dem Zugriff Dritter verbergen kann. Prototypische Entwicklungen zeigen, daß dies mit Verschlüsselungssystemen gelingen kann. Voraussetzung für eine solche Verbesserung des Grundrechtsschutzes mit Hilfe der Informationstechnik ist ein Verschlüsselungsverfahren, das für jedermann verfügbar und für das jeder die benötigten Schlüssel für seine gewünschten Kommunikationspartner erhalten kann. Public-Key-Systeme erfüllen diese Bedingungen, denn die beiden Schlüssel zum Ver- und Entschlüsseln sind verschieden und ohne Zusatzwissen praktisch

nicht gegenseitig ableitbar. Ein Schlüssel des Paares wird dem Teilnehmer „privat" und geheim in einer Chipkarte zur Verfügung gestellt, während der andere in einem Directory, dem „Schlüssel-Telefonbuch", veröffentlicht wird.

Den Verschlüsselungssystemen kommt also mit der zunehmenden Entwicklung von Informationstechniken eine zentrale Bedeutung für die Reduzierung der Verletzlichkeit und der Gewährleistung der Bürgersicherheit zu. Aus diesem Grund erhält das Bundesamt hier die Aufgabe der Forschungs- und Entwicklungsförderung, die auch die Förderung der Anwendung beinhaltet. Die Erforschung, Entwicklung und Anwendung von Verschlüsselungssystemen müssen aber aus Gründen der Verletzlichkeit der Gesellschaft wie der Bürgersicherheit durch unabhängige staatsfreie Einrichtungen erfolgen. Zugriffsmöglichkeiten staatlicher Behörden gefährden die Integrität und damit die Gewährleistung rechtsverbindlicher und vertrauenswürdiger Kommunikation zwischen den Menschen. Aus diesem Grund beschränkt sich die Aufgabe des Bundesamtes auch nur auf die Förderung unabhängiger Forschung, bei der der Staat keinen Einfluß auf den wissenschaftlichen Erkenntnisprozeß und das Ergebnis hat.

Sowohl an das Verschlüsselungsverfahren wie an das Schlüsselmanagement sind allerdings hohe Anforderungen zu stellen. Denn die umfassende Nutzung in der Gesellschaft läßt eine hohe Abhängigkeit des Zahlungssystems und Geschäftsverkehrs von dem verwendeten Publik-Key-System und sensiblen Transaktionen entstehen. Lücken im Sicherungssystem können dann zu hohen materiellen wie immateriellen Schäden für einzelne Bürger oder die gesamte Gesellschaft führen. Das Verschlüsselungsverfahren muß deshalb ausreichend sicher sein, sonst können Teletransaktionen nur noch unter einem hohen Manipulationsrisiko aufgeführt werden. Genauso müssen die geheimen Schlüssel wirklich geheimgehalten werden, sonst können Nachrichten manipuliert, Identitäten vorgetäuscht oder verschlüsselte Nachrichten in den Klartext übersetzt werden. Hier besteht ein großer Forschungs- und Erprobungsbedarf, zu dessen Befriedigung das Bundesamt für die Sicherheit in der Informationstechnik beitragen sollte.

Das Bundesamt für die Sicherheit in der Informationstechnik kann in einem zukunftsorientierten und an der Bürgersicherheit ausgerichteten Handlungskonzept auch selbst wichtige Aufgaben während der Entwicklung und dem Einsatz des Public-Key-System übernehmen: Es sollte die Normung fördern, Fachkompetenz für die öffentliche Diskussion der Vertrauenswürdigkeit des Verfahrens bereitstellen und die verwendeten Systeme validieren.

g) Zu Nummer 4c

Das rechtzeitige Erkennen und Offenhalten von Alternativen zu technischen Entwicklungen trägt dazu bei, die Verletzlichkeit der Gesellschaft zu verringern. Daher soll das Bundesamt für die Sicherheit in der Informationstechnik, wo Bedarf dafür besteht, Modellvorhaben anstoßen und soziale Experimente unterstützen, die Alternativen zur Trendentwicklung in die ‚Informationsgesell-

schaft' darstellen. In solchen Modellversuchen muß das Bundesamt immer auch versuchen, die Gegengewichte gegen die negativen Folgen einer Informatisierungsstrategie zu stärken. Ziel muß es sein, individuelle und soziale Freiräume zu schaffen und vielfältige Alternativen anzubieten.

Für diese Alternativen sind die Verletzlichkeitsaspekte und die von ihnen ausgehenden sozialen, rechtlichen und wirtschaftlichen Folgen abzuschätzen. Da die wissenschaftliche Kapazität zur Durchführung der erforderlichen zukunftsorientierten Implikationsanalysen weitgehend fehlt, ist sie durch entsprechende Nachfrage und den dauerhaften Aufbau von Forschungsmöglichkeiten zu schaffen. Folgenabschätzungen dieser Art sind die Voraussetzung jeder normativen Steuerung des technischen Wandels nach sozialen Kriterien.

h) Zu Nummer 5

Das Bundesamt erhält die Aufgabe einer sachverständigen Unterstützung der sonstigen für die Sicherheit in der Informationstechnik zuständigen Stellen des Bundes. Das Bundesamt soll vor allem auch den Bundesbeauftragten für den Datenschutz bei seiner Tätigkeit unterstützen. Da das Bundesamt nach § 1 Abs. 3 nur der Rechtsaufsicht des Bundesministers des Innern unterliegt und weisungsfrei ist, erübrigt sich ein Hinweis auf die Unabhängigkeit des Bundesbeauftragten für den Datenschutz.

Die Verletzlichkeit der Gesellschaft und die Bürgersicherheit im Bereich der Informationstechnik erfordern eine strikte Trennung zwischen dem Bundesamt und den Geheimdiensten. Die Geheimdienste dürfen durch das Bundesamt nicht unterstützt werden. Gemeint sind damit das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst und der Militärische Abschirmdienst, zu deren Aufgaben beispielsweise auch „technische Sicherheitsmaßnahmen zum Schutz geheimhaltungsbedürftiger Tatsachen, Gegenstände oder Erkenntnisse" gehören (vgl. § 3 Abs. 3 Nr. 3 VerfSchutzG und die Aufgabenbestimmung in Drucksache 11/4306 § 3 Abs. 2 Nr. 3 E-BVerfSchG, § 1 Abs. 4 Nr. 2 E-MADG). Ebensowenig dürfen durch das Bundesamt die Polizeibehörden des Bundes, insbesondere das Bundeskriminalamt, unterstützt werden. Damit beschränken sich die Aufgaben des Bundesamtes im Verschlußsachenbereich auf die Zulassung der Verschlüsselungsgeräte und die Herstellung der Schlüsseldaten.

Das Bundesamt muß, um überhaupt funktionstüchtig für die Unverletzlichkeit der Gesellschaft arbeiten zu können, den Charakter einer „zivilen" Behörde bekommen. Nur unter dieser Voraussetzung kann das Bundesamt das Vertrauen erwerben, das notwendig ist, damit seine Empfehlungen, Warnungen und Anregungen auch praktisch ernstgenommen und umgesetzt werden.

i) Zu Nummer 6

Durch die Streichung der Nummer 6 soll die strikte Trennung der Aufgabenstellung des Bundesamtes gegenüber den Aufgaben der Sicherheitsbehörden erreicht werden. Es zählt nicht zu den Auf-

gaben des Bundesamtes, die Sicherheitsbehörden des Bundes zu unterstützen. Dazu zählen neben dem Bundeskriminalamt auch der Generalbundesanwalt sowie die Geheimdienste. Das Bundesamt soll weder als Klammer zwischen Polizei, Strafverfolgungsbehörden und Geheimdiensten dienen noch durch eine Unterstützung dieser Behörden von diesen für deren Aufgabenerfüllung in Anspruch genommen werden können. Diese institutionelle Entflechtung der Aufgabenstellung des Bundesamtes ist die Konsequenz aus der Unvereinbarkeit des Zwecks des Bundesamtes mit den Aufgaben der Sicherheitsbehörden und ergibt sich aus den Erfordernissen, die Verletzlichkeit der Gesellschaft zu analysieren und zu reduzieren. Das Bundesamt soll dazu beitragen, die Risiken der Informationstechnik für die Bürgersicherheit und die Gesellschaft zu untersuchen und zu reduzieren und dadurch die Rechte der Bürger zu schützen; es ist aber nicht die Aufgabe des Bundesamtes, die Sicherheitsbehörden bei der Wahrnehmung ihrer Aufgaben, die Rechte der Bürger zu beschneiden, zu unterstützen. Die technischen Abteilungen, die zur Unterstützung beispielsweise des Bundeskriminalamtes notwendig sind, müssen daher bei diesem selbst angesiedelt werden.

Außerdem ist die Vorschrift des § 3 Nr. 6 mißglückt, weil die Aufgaben der Verbrechensverhütung, der Strafverfolgung und des Verfassungsschutzes miteinander vermengt werden, für diese aber verschiedene Behörden mit unterschiedlichen Befugnissen zuständig sind. Es zählt beispielsweise nicht zu den Aufgaben des Verfassungsschutzes, Straftaten zu verfolgen, ebensowenig ist es Aufgabe des Generalbundesanwalts, geheimdienstliche Tätigkeiten im Inland zu beobachten. Soweit die Formulierung des Entwurfes eine Unterstützung von Tätigkeiten nichtzuständiger Behörden durch das Bundesamt für die Sicherheit in der Informationstechnik zuläßt, ist sie rechtswidrig.

Unklar bleibt auch die Begrenzung der Unterstützung durch die Formulierung „soweit dies erforderlich ist, um strafbare Handlungen, Bestrebungen oder Tätigkeiten, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen, zu verhindern oder zu erforschen". Behörden des Bundes zur Strafverfolgung sind vor allem der Generalbundesanwalt sowie das Bundeskriminalamt, die selbst nur in ausdrücklich im Gesetz bestimmten Fällen zur Strafverfolgung befugt sind. Einmal abgesehen davon, daß ein Begriff der „Straftaten gegen die Sicherheit in der Informationstechnik" dem geltenden Strafrecht fremd ist, sind diese Bundesbehörden nicht für die Verfolgung der Straftaten gegen die sogenannte Computerkriminalität zuständig. Die Unterstützung des Bundesamtes für die Sicherheit in der Informationstechnik beschränkt sich damit im wesentlichen auf die Verfolgung der Straftaten, die unter Nutzung der Informationstechnologien begangen werden. Im Bereich Verhütung von Straftaten darf das Bundesamt für die Sicherheit in der Informationstechnik im wesentlichen nur das Bundeskriminalamt unterstützen. Das Bundeskriminalamt selbst ist jedoch nur für die „Vorbeugungsarbeit zur Verbrechensbekämpfung" zuständig, soweit es die Polizei der Länder unterstützt. Weitergehende Befugnisse zur Verhütung von Straftaten liegen bei den Ländern.

j) Zu Nummer 7 (unverändert)

k) Zu Nummer 8

Das Bundesamt soll auf Anforderung den Deutschen Bundestag, und damit auch seine Ausschüsse, sowie die Bundesregierung beraten. Diese Aufgabe soll die Vermittlung der bei dem Bundesamt mit der Sicherheit in der Informationstechnologie gemachten Erfahrungen an die Verfassungsorgane gewährleisten. Das Bundesamt steht damit ausdrücklich auch dem Deutschen Bundestag zur Verfügung, soweit es um die Notwendigkeit weiterer gesetzlicher Regelungen zur Verminderung der Verletzlichkeit der Gesellschaft durch die Informationstechnik geht.

l) Zu Nummer 9

Voraussetzung zur Verringerung der Verletzlichkeit der Gesellschaft ist die Ermittlung bisheriger Schadensfälle. Auf diese Weise verfügt das Bundesamt über das notwendige Erfahrungswissen, mit dessen Hilfe die Wahrscheinlichkeit von Schadensfällen, deren Schadensausmaß sowie möglicher Gegenmaßnahmen ermittelt und eine Verringerung der Verletzlichkeit erreicht werden kann.

m) Zu Nummer 10

Mit dem Verletzlichkeitsbericht erhält das Bundesamt die Aufgabe, in einem zusammenfassenden Bericht jährlich über die Entwicklung der Verletzlichkeit der Gesellschaft zu berichten und diese zu bewerten. Das Bundesamt kann damit allen involvierten gesellschaftlichen und staatlichen Instanzen Vorschläge unterbreiten, wie sie durch Technikgestaltung die Verletzlichkeit der Gesellschaft reduzieren können.

Der Verletzlichkeitsbericht richtet sich an den Deutschen Bundestag und die Bundesregierung und ist damit auch der Öffentlichkeit zugänglich. Dies ist eine wichtige Voraussetzung, um besondere Verletzlichkeitsrisiken in einem öffentlichen Diskurs erkennen, bewerten und Gegenmaßnahmen entwickeln zu können.

n) Zu Nummer 11

Das Bundesamt ist als Fachbehörde in Genehmigungs-, Zulassungs- und Planungsverfahren zu beteiligen, deren Gegenstände Auswirkungen auf die Verletzlichkeit der Gesellschaft haben können. Sinn dieser Aufgabenbestimmung ist es, angesichts der wachsenden Bedeutung der Informationstechnik in allen Bereichen der Lebenswelt und der damit einhergehenden Verletzlichkeit der Gesellschaft, dem Bundesamt als Fachbehörde die Möglichkeit zu geben, die Abhängigkeit zu untersuchen und gegebenenfalls durch Vorschläge dazu beizutragen, daß diese gemindert werden. Die Aufgabe der Beteiligung beschränkt sich dabei nicht nur auf die förmlich vorgesehenen Beteiligungsverfahren in Verfahren nach § 73 Abs. 2 VwVfG oder § 10 Abs. 5 BImSchG (Beispiele: Fernmeßanlage zur Verminderung der Emissionen durch den Einsatz der Informationstechnik), sondern auch auf andere Planungsverfahren, wie z. B. TELEKOM oder Beschaffungsprogramme des Bundes.

4. Zu § 3a

(1) Um überhaupt in die Lage versetzt zu werden, die Entwicklung der Verletzlichkeit der Gesellschaft beurteilen zu können, benötigt das Bundesamt für die Sicherheit in der Informationstechnik ausreichende Informationen über die entwickelten und eingesetzten Systeme oder Komponenten der Informationstechnik. Die Anzeigepflicht rechtfertigt sich aber auch aus dem Schutz der Rechte und Interessen der Betroffenen, deren personenbezogene Daten oder sonstige Informationen in informationstechnischen Systemen oder mit Hilfe von Komponenten verarbeitet oder übermittelt werden.

(2) Die Störungsmeldungen ermöglichen dem Bundesamt eine genaue Ermittlung der Abhängigkeit und Verletzlichkeit der Gesellschaft von den jeweils eingesetzten Informationstechniken. Sie bilden die Grundlage für weitere Überlegungen zur Reduzierung der Verletzlichkeit.

Unmittelbare Auswirkungen der Störung sind die Auswirkungen, die in den betriebenen Systemen und Komponenten entstanden sind. Die mittelbaren Auswirkungen beziehen alle darüber hinausgehenden materiellen und immateriellen Schäden beim Betreiber und Dritten mit ein.

(3) Absatz 3 ermöglicht dem Bundesamt weitergehende Befugnisse, wenn die Schadensmeldung unzureichend ist. Mit dieser Befugnis wird gewährleistet, daß Schadensmeldungen, deren Kenntnis für eine Reduzierung der Verletzlichkeit hilfreich sind, nicht unterschlagen werden. Das Bundesamt für die Sicherheit in der Informationstechnik muß über ausreichende Erfahrungsgrundlagen verfügen, um die Risiken rechtzeitig erkennen zu können.

(4) Die noch zu erlassende Rechtsverordnung definiert die informationstechnischen Systeme und Komponenten, die nach Absatz 1 anzeigepflichtig sind, sowie der meldepflichtigen Schäden. Nach Maßgabe der Rechtsverordnung wird dabei, um den jeweiligen Verwaltungsaufwand zu reduzieren, andererseits aber gehaltvolle Anzeigen zu gewährleisten, ein standardisiertes Anzeigeverfahren entwickelt werden. Welche Systeme oder Komponenten anzeigepflichtig sind, ist nach den Kriterien der Verletzlichkeit der Gesellschaft und der Bürgersicherheit zu entscheiden.

Zu beteiligen sind neben Vertretern der Wissenschaft, insbesondere soweit sie sich mit der Sicherheit in der Informationstechnik und deren sozialen und technischen Folgen beschäftigt hat, die Wirtschaft als Hersteller, Vertreiber und Anwender der Informationstechnik sowie die Betroffenen bzw. deren Vertreter. Zu den Betroffenen der Informationstechnik zählen die Menschen, die mit der Informationstechnik arbeiten, deren Daten oder Informationen mit ihrer Hilfe verarbeitet werden, oder die als Verbraucher sonst durch Auswirkungen der Informationstechnik berührt werden können.

(5) Ausgenommen von der Anzeigepflicht sind aus kompetenzrechtlichen Gründen lediglich die Behörden der Länder und der Gemeinden, denen jedoch eine freiwillige Anzeige unbenommen bleibt. Die Gesetzgebungskompetenz des Bundes für die Einfüh-

rung der Anzeigepflicht Privater ergibt sich aus Artikel 74 Nr. 11 GG (Wirtschaft).

5. Zu § 3b

Die Dokumentation besteht aus einer Datei mit den Angaben aus den Anzeigen nach § 3a Abs. 1 und 2. Zweck der Dokumentation ist es, das Ausmaß der Abhängigkeit von der Informationstechnik erkennen und Gegenmaßnahmen entwickeln zu können. Dazu können beispielsweise die Schadensanzeigen mit den Anzeigen über die hergestellten und eingesetzten Systeme korreliert werden. Die Auswertung der Anzeigen erlaubt die zielgerichtete Vergabe von Forschungsaufträgen, die Entwicklung von Sicherheitskomponenten, die Festlegung von Anordnungen zur technischen und organisatorischen Gestaltung der informationstechnischen Systeme und Komponenten sowie die gezielte Beratung und Warnung der Hersteller, Vertreiber und Betreiber der informationstechnischen Systeme oder Komponenten

Im Register sind nur die allgemeinen Angaben aus den Anzeigen enthalten. Eine Beeinträchtigung von Betriebs- und Geschäftsgeheimnissen kann daher ausgeschlossen werden. Soweit der Meldepflichtige eine natürliche Person ist, sind seine Daten faktisch zu anonymisieren (§ 16 Abs. 6 BStatG). Das Einsichtsrecht dient der Information potentiell Betroffener über mögliche Risiken der verwendeten Informationstechnik.

(2) Eine der wichtigsten Aufgaben des Bundesamtes für die Sicherheit der Informationstechnik besteht darin, in der Öffentlichkeit Problembewußtsein zu schaffen, die Beurteilungskompetenz zu stärken und Gestaltungswissen zu vermitteln. Daher ist das Bundesamt verpflichtet, die Auswertung der Anzeigen zu veröffentlichen. Sie kann gemeinsam mit dem Verletzlichkeitsbericht erfolgen. Darüber hinaus gibt die Veröffentlichung typischer Schadensfälle dem Anwender Gelegenheit, die Sicherheit ihres Informationssystems zu überprüfen und zu verbessern.

(3) Darüber hinaus muß das Bundesamt die von ihm initiierten Studien veröffentlichen, damit eine informierte Diskussion über die Verletzlichkeit der Gesellschaft und der Bürgersicherheit möglich ist.

6. Zu § 3c

Der Verletzlichkeitsbericht gibt dem Bundesamt die Möglichkeit, zusammenfassend den Entwicklungsstand der Informationstechniken, die dabei auftretenden Probleme sowie die Abhängigkeit der Gesellschaft von der Informationstechnik zu beschreiben und zu bewerten. Dabei wird das Bundesamt sowohl das Problembewußtsein einer breiten Öffentlichkeit anregen als auch gleichzeitig mögliche Alternativen und Gegenmaßnahmen skizzieren.

Gleichzeitig ermöglicht der Verletzlichkeitsbericht Bundestag und Bundesregierung, sich gegenüber der Öffentlichkeit mit der Verletzlichkeit der Gesellschaft durch die Entwicklung der Informationstechnik auseinanderzusetzen und entsprechende Gegenmaßnahmen zu ergreifen.

7. Zu § 3d

(1) Das Instrument der Empfehlung dient der Berücksichtigung der Verletzlichkeit in Planungsentscheidungen und ermöglicht es den Behörden des Bundes, sich des Sachverstandes des Bundesamtes zu vergewissern und mit ihm auseinanderzusetzen. Dadurch kann das Erfahrungswissen von anderen Behörden gezielt zur Verminderung möglicher Kosten bei Schadensfällen und insgesamt der Verletzlichkeit eingesetzt werden. Das Bundesamt kann sich aber auch von sich aus in Verfahren wie beispielsweise Beschaffungsprogramme des Bundes einschalten.

Die Verletzlichkeit der Gesellschaft erfordert eigentlich weitergehende Genehmigungs- und Zulassungsverfahren nach Maßgabe präventiver Kontrolle. In solchen Verfahren wären allerdings nicht nur Verletzlichkeitsprüfungen durchzuführen, sondern es wären vielmehr weitere Gesichtspunkte wie Datenschutz, Verfassungsverträglichkeit, Arbeitsschutz, Verbraucherschutz zu berücksichtigen. Angesichts der Komplexität derartiger Regelungen sind sie einem eigenen Gesetz zur Kontrolle der Informationstechnik vorzubehalten und nicht in das Gesetz zur Errichtung eines Bundesamtes für die Sicherheit in der Informationstechnik aufzunehmen.

(2) Das Mittel der Anordnungen ermöglicht es dem Bundesamt, in den Fällen, in denen die Erfordernisse der Sicherheit in der Informationstechnik unvertretbar vernachlässigt werden, einzugreifen. Diese Befugnis gilt gegenüber Behörden und Unternehmen des Bundes sowie Privaten. Voraussetzung ist allerdings, daß unvertretbare Risiken für die Gesellschaft oder Dritte geschaffen und diesen nicht abgeholfen wird.

8. Zu § 3e

Die Beurteilung der Risiken und die Bewertung von Schutzmaßnahmen ist weitgehend von subjektiven Wertungen abhängig. Gerade deshalb ist es erforderlich, den Gefahren möglicher einseitiger Bewertungen durch institutionalisierte kritische Diskurse zu begegnen. Diese sollten eine kontroverse Reflexion über die Verletzlichkeit wichtiger Technikanwendungen in Gang bringen. Sie sollten jedoch nicht auf einen vorschnellen Konsens zielen, sondern vielmehr einer kritischen Aufarbeitung der Verletzlichkeitsrisiken dienen.

Zu diesem Zweck wird beim Bundesamt für die Sicherheit in der Informationstechnik ein Beirat eingerichtet, dessen Aufgabe in der begleitenden Diskussion der Arbeit des Bundesamtes besteht. Um dieser Aufgabe gerecht zu werden, ist der Beirat wissenschaftlich interdisziplinär und mit Vertretern verschiedener betroffener Gruppen besetzt.

Die Sicherheit in der Informationstechnik kann nicht einer einzigen wissenschaftlichen Disziplin zugeordnet werden, vielmehr bedarf eine begleitende Diskussion durch den Beirat auch einer entsprechenden interdisziplinären Zusammensetzung der Wissenschaftler. Angesprochen sind damit die Wissenschaftsbereiche der Sicherheitstechnik und damit sowohl die Ingenieurswissen-

schaften als auch die Informatik, der Technikfolgenabschätzung und der Sozialverträglichkeit.

Die Mitgliedschaft des Bundesbeauftragten für den Datenschutz rechtfertigt sich aus den Gefahren, die sich aus der Anwendung der Sicherheitstechnik für die Persönlichkeitsrechte der Betroffenen ergeben.

Die Vertreter der Hersteller sollten sowohl aus dem Bereich der Software als auch der Hardware kommen. Ihre Mitgliedschaft kann dazu beitragen, das bereits bei der Konstruktion und Herstellung der informationstechnischen Systeme und Komponenten durch entsprechende technische Implementationen die Verletzlichkeit vermindert werden kann.

Die Teilnahme von weiteren Vertretern der Wirtschaftsverbände begründet sich aus der Betroffenheit der Wirtschaft als Anwender der Informationstechnik gegenüber Dritten sowie als Eigennutzer gegenüber den Herstellern. Die Verletzlichkeit macht sich ihnen gegenüber durch ein großes Schadensausmaß im Schadensfall bemerkbar.

Die Verbraucherverbände vertreten die Endbetroffenen, die als Käufer oder Nutzer der Informationstechnik betroffen sind. Verbraucher sind aber auch dadurch betroffen, weil Dienstleistungsunternehmen ihnen gegenüber Informationstechnik anwenden. Verbraucher spüren in der Regel die Auswirkungen der Informationstechnik, sei es als soziale oder wirtschaftliche Auswirkungen, zuerst.

Die Auswirkungen der Informationstechnik beschränken sich aber nicht nur auf die Nutzer und Anwender, sondern machen sich auch bei den Beschäftigten der Unternehmen bemerkbar, die mit der Informationstechnik arbeiten. Aus diesem Grund sind auch zwei Gewerkschaftsvertreter im Beirat vertreten.

Bürgerrechtsgruppen vertreten die Interessen der Bürger/innen dort, wo Sicherungsmaßnahmen negative Folgen für die Grundrechtsausübung des einzelnen und das soziale und politische System insgesamt hervorrufen.

Frauengruppen vertreten die Interessen der Frauen, die sich mehrheitlich eine größere Sensibilität und größeres Verantwortungsbewußtsein gegenüber den schädlichen Auswirkungen der IuK-Technik bewahrt haben.

9. Zu § 5a

Der Präsident des Bundesamtes wird vom Deutschen Bundestag gewählt, er verfügt damit über eine demokratische Legitimation. Seine Qualifikation wird vorher in einer Anhörung des Bundestagsausschusses, bei der die Kandidaten befragt werden, festgestellt. Das Vorschlagsrecht liegt bei der Bundesregierung.

10. Zu § 6 (unverändert)

11. Zu § 6a

Diese Norm dient zur Durchsetzung der Pflicht nach § 3 Abs. 1 bis 3.

Druck: Thenée Druck KG, 5300 Bonn, Telefon 23 19 67
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 13 63, Herderstraße 56, 5300 Bonn 2, Telefon (02 28) 36 35 51, Telefax (02 28) 36 12 75
ISSN 0722-8333